

- [120] H. Aghakhani, F. Gritti, F. Mecca, M. Lindorfer, S. Ortolani, D. Balzarotti, G. Vigna, and C. Kruegel, “When Malware is Packin’ Heat; Limits of Machine Learning Classifiers Based on Static Analysis Features,” in *27th Annual Network and Distributed System Security Symposium, NDSS 2020, San Diego, California, USA, February 23-26, 2020*, The Internet Society, 2020.
- [121] M. W. J. Chua and V. Balachandran, “Effectiveness of Android Obfuscation on Evading Anti-malware,” in *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy, CODASPY*, pp. 143–145, 2018.
- [122] P. Dasgupta and Z. Osman, “A Comparison of State-of-the-art Techniques for Generating Adversarial Malware Binaries,” *CoRR*, vol. abs/2111.11487, 2021.
- [123] G. Lu and S. K. Debray, “Weaknesses in Defenses against Web-borne Malware - (Short Paper),” in *Proceedings of Detection of Intrusions and Malware, and Vulnerability Assessment - 10th International Conference, DIMVA 2013*, vol. 7967, pp. 139–149, Springer, 2013.
- [124] M. Payer, “Embracing the New Threat: Towards Automatically Self-diversifying Malware,” in *Proceedings of The Symposium on Security for Asia Network*, pp. 1–5, 2014.
- [125] N. Loose, F. Mächtle, C. Pott, V. Bezsmertnyi, and T. Eisenbarth, “Madvex: Instrumentation-based Adversarial Attacks on Machine Learning Malware Detection,” in *Detection of Intrusions and Malware, and Vulnerability Assessment - 20th International Conference, DIMVA 2023*, vol. 13959 of *Lecture Notes in Computer Science*, pp. 69–88, 2023.
- [126] R. Sasnauskas, Y. Chen, P. Collingbourne, J. Ketema, J. Taneja, and J. Regehr, “Souper: A Synthesizing Superoptimizer,” *CoRR*, vol. abs/1711.04422, 2017.
- [127] B. G. Ryder, “Constructing the Call Graph of a Program,” *IEEE Transactions on Software Engineering*, no. 3, pp. 216–226, 1979.
- [128] S. Narayan, C. Disselkoen, D. Moghimi, S. Cauligi, E. Johnson, Z. Gang, A. Vahldiek-Oberwagner, R. Sahita, H. Shacham, D. M. Tullsen, and D. Stefan, “Swivel: Hardening WebAssembly against Spectre,” in *30th USENIX Security Symposium, USENIX Security 2021, August 11-13, 2021*, pp. 1433–1450, 2021.
- [129] E. Johnson, D. Thien, Y. Alhessi, S. Narayan, F. Brown, S. Lerner, T. McMullen, S. Savage, and D. Stefan, “SFI Safety for Native-compiled Wasm,” *NDSS. Internet Society*, 2021.

- [130] M. Willsey, C. Nandi, Y. R. Wang, O. Flatt, Z. Tatlock, and P. Panchekha, “Egg: Fast and Extensible Equality Saturation,” *Proc. ACM Program. Lang.*, vol. 5, no. POPL, pp. 1–29, 2021.
- [131] “Stop a wasm compiler bug before it becomes a problem | fastly.” <https://www.fastly.com/blog/defense-in-depth-stopping-a-wasm-compile-r-bug-before-it-became-a-problem>, 2021.
- [132] D. Cao, R. Kunkel, C. Nandi, M. Willsey, Z. Tatlock, and N. Polikarpova, “babble: Learning Better Abstractions with E-Graphs and Anti-unification,” *Proc. ACM Program. Lang.*, vol. 7, no. POPL, pp. 396–424, 2023.
- [133] R. Tate, M. Stepp, Z. Tatlock, and S. Lerner, “Equality Saturation: A New Approach to Optimization,” in *Proceedings of the 36th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL*, pp. 264–276, 2009.
- [134] T. D. Morgan and J. W. Morgan, “Web Timing Attacks Made Practical,” *Black Hat*, 2015.
- [135] T. Schnitzler, K. Kohls, E. Bitsikas, and C. Pöpper, “Hope of Delivery: Extracting User Locations From Mobile Instant Messengers,” in *30th Annual Network and Distributed System Security Symposium, NDSS 2023, San Diego, California, USA, February 27 - March 3, 2023*, The Internet Society, 2023.
- [136] Mozilla, “Protections Against Fingerprinting and Cryptocurrency Mining Available in Firefox Nightly and Beta ,” 2019.
- [137] F. Cohen, “Computer Viruses: Theory and Experiments,” *Comput. Secur.*, vol. 6, no. 1, pp. 22–35, 1987.
- [138] P. Kocher, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, M. Schwarz, and Y. Yarom, “Spectre Attacks: Exploiting Speculative Execution,” *meltdownattack.com*, 2018.
- [139] M. Schwarz, C. Maurice, D. Gruss, and S. Mangard, “Fantastic Timers and Where to Find Them: High-resolution Microarchitectural Attacks in JavaScript,” in *Financial Cryptography and Data Security - 21st International Conference, FC*, vol. 10322, pp. 247–267, 2017.
- [140] G. J. Duck, X. Gao, and A. Roychoudhury, “Binary Rewriting Without Control Flow Recovery,” in *Proceedings of the 41st ACM SIGPLAN International Conference on Programming Language Design and Implementation, PLDI*, pp. 151–163, 2020.